

WHAT IS CLAIMED IS:

1. An information protection system comprising a storage medium to be loaded on an external device, the storage medium including a storage portion for storing information data and at least predetermined application program data for controlling the external device, an electronic circuit portion for controlling the external device based on the data and the application program that are read out of the storage portion, and also permission information for controlling whether to permit or refuse access to the storage portion so that, at the time of accessing by the external device to the storage medium, such access is enabled only if permitted based on the permission information.

2. An information protection system comprising a plurality of external devices each loaded with a storage medium including a storage portion in which information data and at least a predetermined application program for controlling an external device are stored, an electronic circuit portion for reading out the data and controlling the external device based on the read-out application program, and permission information stored in the storage portion for controlling whether permit or refuse access to the storage portion in such a manner that some of the permission information stored in the storage media are different from the others, and at the time of accessing to the storage medium by the external device, such access is enabled only if permitted based on the permission information.

3. In a network system comprising an independent network having a PC connected to a dedicated line and a normal network connected to internet and having a plurality of PCs connected to a LAN,

an information protection system characterized in that each of the PCs connected to the normal network is loaded with a storage medium having a storage portion for storing information data and predetermined application program data for controlling at least the PC, an electronic circuit portion for reading out the data from the storage portion and controlling the PC based on the read-out application program, and permission information stored in the

storage portion for controlling whether permit or refuse access to the storage portion so that at the time of accessing the storage medium by the PC, such access is permitted only if permitted based on the permission information.

4. An information protection system comprising a storage case for storage of a plurality of storage media each having a storage portion for storing information data and predetermined application program data for controlling at least a PC, an electronic circuit portion for reading out the data from the storage portion and controlling the external device based on the read-out application program, and permission information stored in the storage portion for controlling whether permit or refuse access to the storage portion in such a manner that a particular storage medium is enabled to be taken out of the storage case only if he/she is certified as one of previously registered particular persons,

wherein the taken-out storage medium is loaded in the external device and, at the time of access to the storage medium by the external device, such access is enabled only if permitted based on the permission information.

5. An information protection system comprising a storage case for storing a plurality of storage media each having a storage portion for storing information data and predetermined application program data for controlling at least an external device, an electronic circuit portion for reading out the data from the storage portion and controlling the external device based on the read-out application program, and permission information stored in the storage portion for controlling whether permit or refuse access to the storage portion in such a manner that a predetermined storage media are enabled to be taken out of the storage case only if he/she is certified as one of previously registered particular persons,

wherein the taken-out storage media are loaded in the plurality of external devices, the permission information stored in some of the storage media are different from others, and at the time of accessing to the storage media by the external devices, such access is enabled only if permitted based on the permission information.

6. In a network system comprising an independent network having a PC connected to a dedicated line and a normal network having a plurality of PCs connected to a LAN and also connected to internet,

an information protection system comprising a storage case for storing a storage medium to be connected to each PC in the normal network and having a storage portion for storing information data and predetermined application program data for controlling at least the PC, an electronic circuit portion for reading out the data from the storage portion and controlling the PC based on the read-out application program, and permission information stored in the storage portion for controlling whether permit or refuse access to the storage portion in such a manner that the predetermined storage medium is enabled to be taken out of the storage media storage case only if he/she is certified as one of previously registered particular persons,

wherein the taken-out storage medium is loaded in an external device and at the time of accessing the storage medium by the PCs, such access is enabled only if permitted based on the permission information.

7. An information protection system of either one of claims 1 to 6, wherein the external device is a PC connected to internet.

8. An information protection system of either one of claims 4 to 6, further comprising means for generating warning when the storage medium is taken out despite NG in the certification result.

9. An information protection system of either one of claims 4 to 6, further comprising means for generating warning when the storage medium is taken out and brought outside a predetermined area despite NG in the certification result.

10. An information protection system of claim 8 or 9, wherein the warning is sent to a control center by way of a communication line.

11. An information protection system of claim 2 or 5, wherein some of the permission information stored in the storage media as loaded in a plurality of external devices are different from others.

12. An information protection system of either one of claims 1 to 11, the information data stored in the storage medium are encrypted and the permission information is information for decrypting the encryption.

13. An information protection system of either one of claims 1 to 12, wherein the storage medium is an optical disc.

14. A storage medium to be detachably loaded in an external device and having a storage portion for storing information data and predetermined application program data for controlling at least the external device, an electronic circuit portion for reading out the data from the storage portion and controlling the external device based on the read-out application program, and permission information for controlling whether permit or refuse access to the storage portion.

15. A storage medium of claim 14, wherein the information data stored in the storage medium is encrypted and the permission information is information for decrypting the encryption.

16. A storage medium drive unit capable of accessing to the storage portion of the storage medium of claim 14 or 15 and further comprising a drive having an interface portion for communicating with the electronic circuit portion as an integral part with the storage medium.

17. A storage media storage case for storing a plurality of the storage media or the storage medium drive units of claim 14 or 15 and for enabling a person to take out a predetermined storage medium or the storage medium drive unit only if he/she is certified as one of previously registered particular persons.

18. A storage media storage case of claim 16, wherein the certification is either ID or a biometric identification.

19. A storage media storage case of claim 17 or 18, further comprising means for generating warning when the storage medium is taken out despite NG in the certification result.

20. A storage media storage of either one of claims 17 to 19, further comprising means for generating warning when the storage medium is taken out and brought outside a predetermined area despite NG in the certification result.

21. A storage media storage case of claim 19 or 20, wherein the warning is either a warning sound or a warning display.

22. A storage media storage case of either one of claims 19 to 21, wherein the warning is transmitted to a control center by way of a communication line.

23. A storage media storage case of either one of claims 17 to 22, wherein the storage media are optical discs.

24. An information protection system, a storage medium or a storage media storage case of either one of claims 1 to 23, wherein the storage medium is accommodated in a cartridge.

25. An information protection system, a storage medium or a storage media storage case of either one of claims 1 to 23, wherein the cartridge is capable of accommodating any storage medium.

26. An information protection system, a storage medium or a storage media storage case of claim 24 or 25, wherein the cartridge includes a wireless communication portion for making wireless communication, an identification portion, a display portion, an audio output portion and a battery portion for driving these functional portions.

27. An information protection system, a storage medium or a storage media storage case of claim 25, wherein the location of the cartridge is controlled by making wireless communication of the wireless communication portion, an alarm is generated when the cartridge is brought outside a predetermined area, and the alarm is transmitted to a control center by way of a wireless communication network for notifying the abnormality.

28. An information protection system, a storage medium or a storage media storage case of claim 27, wherein the identification portion installed in the cartridge generates an alarm or notifies to the control center when a person who tries to take out the cartridge is not a registered person permitted to use (NG in certification).

29. An information protection system, a storage medium or a storage media storage case of claim 27, wherein justification of the storage medium is confirmed by communication between the wireless communication portion in the cartridge and the wireless communication portion as provided at the storage medium side.

30. An information protection system, a storage medium or a storage media storage case of either one of claim 24 to 29, wherein the storage medium is an optical disc.